

FILED

June 19, 2020

Sealed
Public and unofficial staff access
to this instrument are
prohibited by court order

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

David J. Bradley, Clerk of Court

United States of America

v.

Joseph Cohen aka "User 2"

Case No. **4:20-mj-1099**

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of July 2018 to present in the county of Harris in the
Southern District of Texas, the defendant(s) violated:

Code Section

Offense Description

18 U.S.C. 2252A(a)(2) and (b)(1)


Conspiracy to Receive and Distribute Child Pornography

18 U.S.C. 2251(d) and (e)

Conspiracy to Advertise Child Pornography

This criminal complaint is based on these facts:

See attached affidavit

☒ Continued on the attached sheet.


Complainant's signature

Joshua Conrad / Special Agent

Printed name and title

Sworn to before me telephonically.

Date: June 19, 2020City and state: Houston, Texas


Judge's signature

Dena Hanovice Palermo, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Joshua Conrad, a Special Agent with Homeland Security Investigations, being duly sworn, depose, and state as follows:

INTRODUCTION

1. I am a Special Agent (“SA”) with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (“HSI”), assigned to the Special Agent in Charge in Philadelphia, PA, and I have been so employed since April 2016. Prior to that, I was assigned to the Special Agent in Charge in El Paso, Texas, since October 2010. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A. I have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants, a number of which involved child exploitation and/or child pornography offenses.

2. This affidavit is made in support of a criminal complaint charging Joseph COHEN with: 1) Conspiracy to receive and distribute child pornography in violation of 18 U.S.C. §§ 2252A(a)(2) & 2252A(b)(1) and 2) Conspiracy to advertise child pornography in violation of 18 U.S.C §§ 2251(d) & (e).

3. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted and based on my conversations with other law enforcement officers who have engaged in numerous investigations involving child exploitation, and with other witnesses.

4. Because this Affidavit is being submitted for the limited purpose of demonstrating probable cause in support of the attached criminal complaint, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause.

STATUTORY AUTHORITY

5. Title 18 U.S.C. § 2252A(a) and (b)(1) prohibits a person from knowingly transporting, shipping, receiving, distributing, reproducing for distribution, possessing, or accessing with intent to view any child pornography, as defined in Title 18 U.S.C. § 2256(8), when such child pornography was either mailed or shipped or transported in interstate or foreign commerce, or in or affecting interstate commerce, by any means, including by computer, or when such child pornography was produced using materials that had traveled in interstate or foreign commerce, and any attempts or conspiracies to do so.

6. Title 18 U.S.C. § 2251(d) prohibits a person from knowingly making, printing, publishing, causing to be made, printed, or published, any notice or advertisement seeking or offering to receive, exchange, buy, produce, display, distribute, or reproduce any visual depiction the production of which involved the use of a minor engaging in sexually explicit conduct if that person knows or has reason to know that the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer, or such notice or advertisement is transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer, any attempts or conspiracies to do so.

PROBABLE CAUSE

Investigation of Network 1, Network 2, and Network 3

7. On or about May 31, 2017, HSI SA Joshua Conrad created the undercover online identity, “UC1,”¹ to access Protocol A² chat rooms on the Network 1³ network. Protocol A chats are applications that facilitate communication by text. Protocol A chat rooms are mainly designed for group communication in discussion forums, but can also be used for private, one-on-one communications, data sharing, and file sharing.

8. SA Conrad, while in the Eastern District of Pennsylvania, used the UC1 undercover online identity to join and access multiple Protocol A Network 1 chat rooms, all of which were forums in which potential targets expressed interest in engaging in sexual activities with minors and/or trafficking in sexually explicit depictions of minors.

9. While SA Conrad was logged into “Chat Room 1”⁴ on the Network 1 server, SA Conrad observed a user, “User 1,”⁵ posting links to third-party file-sharing websites. SA Conrad accessed several of these links and confirmed that the links led to child pornography images, including nude prepubescent girls engaged in oral, vaginal, and anal sex with adult men as well

¹ The real user name of UC1 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

² The real name of Protocol A is known to law enforcement but is being disguised in order to protect the ongoing investigation.

³ The real name of Network 1 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

⁴ The real name of Chat Room 1 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

⁵ The real user name of User 1 references the sexual exploitation of children. The real user name is known to law enforcement but is being disguised in order to protect the ongoing investigation.

as nude prepubescent girls in various poses exposing their vaginas and anuses. SA Conrad also observed User 1 changing chat room modes for other users, which indicated User 1 had chat room administrative rights for Chat Room 1 on Network 1. Within Protocol A there are numerous chat room modes that function essentially as rules for how a chat room operates. For example, there is a chat room mode that can ban users with a particular nickname from joining a chat room, and there is a chat room mode which makes the chat room invite-only. Other users in Chat Room 1 could see User 1's user name. This user name is the Protocol A user name that User 1 designated as the name to display when that user was connected to Protocol A.

10. Protocol A has two tiers of administrators, a higher tier and a lower tier. The lower tier administrator has the ability to manage and control users and issues at the chat room level. The higher tier administrator has the ability to manage and control users and issues at the network level. The User 1 user, whose user name is indicative of a sexual interest in children, was a member of both moderator tiers. User 1 also had a bot—a computer program that performs automatic, repetitive tasks—set up that automatically posted to Chat Room 1 a link to a third-party file sharing-website once per minute. The majority of these links lead to third-party sites displaying an image or video of prepubescent minors engaging in sexually explicit conduct, much of which SA Conrad has downloaded and preserved for evidentiary purposes.

Transition from Network 1 to Network 2

11. Protocol A's network administrators and moderators are charged with the task of enforcing a particular network's rules and, in many cases, improving the network in various ways. In or about July 2018, several Network 1 administrators began closing Network 1 chat rooms focused on child sexual exploitation material, including Chat Room 1 and "Chat Room

2,”⁶ to name a few. On or about July 26, 2018, a post was made to the website “textuploader.com” informing users of a new private Protocol A server, known as “Network 2,”⁷ and how to access it. The post discussed how the new Network 2 was a private Protocol A network offering a secure encrypted connection between a server and a web browser, the ability to mask a user’s IP address information, and the ability to register a unique user name. The post then provided detailed instructions on how to set up and access Network 2 using the Protocol A client.

12. SA Conrad observed that, around the time the Network 1 administrators began eliminating chat rooms dedicated to trafficking in child sexual exploitation material, the users who most frequently posted links to child sexual exploitation material on Network 1, like User 1, migrated from Network 1 over to the newly-created Network 2, where many of the chat rooms dedicated to trafficking in child sexual exploitation material that had been banned on Network 1—such as Chat Room 1, Chat Room 2, and “Chat Room 3”⁸—had been recreated.

13. On September 28, 2018, SA Conrad logged onto Network 2 and was presented with a welcome message for Network 2. The welcome message listed the “Staff Members” associated with Network 2. One user, “User 2,”⁹ was listed as a “Network Admin” of Network 2,

⁶ The real name of Chat Room 2 is sexually explicit and references the sexual exploitation of children. The real name is known to law enforcement but is being disguised in order to protect the ongoing investigation.

⁷ The real name of Network 2 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

⁸ The real name of Chat Room 3 is sexually explicit and references the sexual exploitation of children. The real name is known to law enforcement but is being disguised in order to protect the ongoing investigation.

⁹ The real user name of User 2 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

meaning that that user would have had full network administrative privileges over that Network. (The individual believed to be User 2 is the subject of this criminal complaint, as will be demonstrated in greater detail below.)

14. On or about September 28, 2018, at approximately 17:03 hours ET, User 2 was logged into Chat Room 1 on Network 2. While User 2 was logged in, User 1's bot posted a link to a third-party website which, when clicked, lead to an image of a naked prepubescent female laying on a blue carpet exposing her vagina. This link would have been available to any user logged onto Chat Room 1 on Network 2 at the time, including User 2. SA Conrad downloaded this image for evidentiary purposes. While User 2 was logged in, User 1's bot posted another link to a third-party website which, when clicked, lead to a close-up image of a naked prepubescent girl's vagina and a "LS Models"¹⁰ watermark stamped in the upper-left corner of the image. This link would have been available to any user logged onto Chat Room 1 on Network 2 at the time, including User 2. SA Conrad downloaded this image for evidentiary purposes.

15. On or about October 18, 2018, at approximately 02:15 hours ET, User 2 was logged into Chat Room 1 on Network 2. While User 2 was logged in, User 1's bot posted a link to a third-party website which, when clicked, lead to an image of a naked prepubescent female standing on a red carpet with her exposed vagina. This link would have been available to any user logged onto Chat Room 1 on Network 2 at the time, including User 2. SA Conrad downloaded this image for evidentiary purposes. At approximately 02:46 hours ET, while User 2 was logged in, User 1's bot posted another link to a third-party website which, when clicked,

¹⁰ Your affiant knows, based on his training and experience, that "LS Models" is a well-known child pornography series.

lead to a closeup image of a naked prepubescent girl's vagina with the "LS Models" watermark stamped in the upper-right corner of the image. This link would have been available to any user logged onto Chat Room 1 on Network 2 at the time, including User 2. SA Conrad downloaded this image for evidentiary purposes.

Transition from Network 2 to Network 3

16. On or about February 19, 2019, at approximately 10:48 hours ET, in the Eastern District of Pennsylvania, SA Conrad logged into the Network 2 server in an undercover capacity. SA Conrad noticed that there were significantly fewer users logged in to Chat Room 1, typically the most populated, than he had observed during prior undercover sessions. At approximately 10:55 hours ET, a post was made to Chat Room 1 by "[User 1]-afk",¹¹ which stated the following, "We would like to inform everyone that [Network 2] will be closing soon for technical reasons. We invite everyone to join us at our new server" and then listed precise technical instructions for joining a new server named "[Network 3]".¹² SA Conrad accessed Network 3 using the given instructions and thereafter observed a welcome screen for Network 3 that emphasized its lack of content oversight.

17. Around this time, SA Conrad again observed that, as with the earlier transition from Network 1 to 2 described above, the users who most frequently posted links to child sexual exploitation material, like User 1, had migrated from Network 2 over to the newly-created Network 3, where many of the chat rooms that had existed on Network 2 had again been

¹¹ In your affiant's training and experience, in Internet parlance, "afk" stands for "away from keyboard." User 1 often wrote posts that were automatically posted to the chat room, even though he may not have been physically be in front of the computer at that time.

¹² The real name of Network 3 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

recreated with the same names they had on Network 2. Through my investigation, your affiant has learned the following regarding the real identities of User 1 and User 2:

Identification of User 1

18. On August 28, 2019, HSI agents executed a federal search warrant at the residence of Charles McCREARY located in the Southern District of Texas. At the time of the execution of the warrant, agents encountered McCreary. McCreary admitted, in a post-*Miranda* interview, that he was User 1 on Networks 1, 2, and 3 on Protocol A.

Identification of User 2 aka Joseph COHEN

19. On or about August 28, 2019, HSI agents executed five virtually simultaneous search warrants on five individuals who had acted as either moderators or network administrators for Network 2 and/or Network 3. During a search of the home of one of those individuals—hereafter referred to as “User 3”¹³—law enforcement seized several devices containing evidence related to child sexual exploitation offenses that had occurred on Protocol A networks. The investigation revealed that User 3 was a network administrator for Network 2 and Network 3. One of the devices seized from User 3’s home yielded network administrator log files for Networks 2 and 3 that documented, among other things, chat conversations between administrators, including User 2 and User 3, as well as other user data that would later be used to help identify what is believed to be User 2’s real-world identity (as discussed in greater detail below).

20. The investigation revealed that network administrators for Networks 2 and 3 created several chat rooms that are only accessible to the network administrators. The network

¹³ The real user name of User 3 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

administrators used these administrative chat rooms to assist them in monitoring the networks, the various chat rooms within the networks, user data, and any requests from other network users. “Network Admin Chat Room 1”¹⁴ is a chat room that existed on both networks that allowed the network administrators to have group chat conversations among themselves. A second such chat room, “Network Admin Chat Room 2,”¹⁵ is a chat room that existed on both networks that allowed the network administrators to monitor when users joined or quit the network or a particular chat room within it. Network Admin Chat Room 2 also kept a log of the true IP addresses of the users logging in to the networks—that is, the IP address that corresponded to that user’s actual physical location (unless the IP address was otherwise disguised by the user). A third such chat room, “Network Admin Chat Room 3,”¹⁶ that existed on both networks, allowed the network administrators to monitor and respond to help requests made by regular network users.

21. SA Conrad reviewed information within the Network 2 Admin Chat Room 1 logs seized from User 3’s devices in order to search for information that could be used to identify the real-world identity of User 2. As discussed above, these logs contained private chat conversations between the Network 2 administrators and were only accessible by Network 2

¹⁴ The real user name of the Network Admin Chat Room 1 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

¹⁵ The real user name of the Network Admin Chat Room 2 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

¹⁶ The real name of the Network Admin Chat Room 3 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

administrators. These logs showed that another particular user, “User 4,”¹⁷ was considered the so-called owner of Network 2. This meant that this member had decision-making authority and founding member status in the Network 2 community. The investigation revealed that User 4 was responsible for paying to make sure that Network 2 continued to function. SA Conrad also learned that Network 2 was hosted on a server that was leased by a company owned by another particular user, “User 5,”¹⁸ called “NXT Gaming Solutions.” Through the course of the investigation and the review of the seized administrator chat logs, SA Conrad also learned that several of the administrators would pay User 4 via PayPal to maintain the functionality of and access to Network 2. On or about September 5, 2018, at approximately 15:21 hours ET, User 4 told the members of the Network 2 Admin Chat Room that they had a new contributor, User 2. He then said the following about User 2: “I would like to introduce you to NXT Gaming Solutions new financial investor. aka [User 2] >.<”¹⁹ The logs also showed that User 2 was made a network administrator for Network 2 that same day and that he began performing administrative functions, such as removing problem users from the chat rooms, at that time.

22. During an interview of User 5, conducted around the time a search warrant was executed at his residence, User 5 was asked about User 4 and about how financial contributions to Network 2 were made. User 5 explained the process and provided to the agents the email address associated with the PayPal account User 4 utilized to maintain Network 2, namely: “bigstevedw@hotmail.co.uk.” User 5 also explained that members of the network would

¹⁷ The real user name of User 4 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

¹⁸ The real user name of User 5 is known to law enforcement but is being disguised in order to protect the ongoing investigation.

¹⁹ All spelling and grammar errors in direct quotations are presented as found in the original communications.

occasionally pay him, his company, or User 4 for the expenses incurred for running the network and/or leasing the server on which Network 2 was hosted. On or about September 23, 2019, SA Conrad served a summons on PayPal for information about transactions related to the email address User 5 provided. PayPal responded with transaction logs pertaining to the account that was associated with the email address User 5 said belonged to User 4.

23. SA Conrad learned from these PayPal logs that, on or about September 8, 2018, there was a payment from one “Joseph Lerner” in the amount of \$13.52 to the PayPal account associated with User 4 and the “bigsetevedw@hotmail.co.uk” email address. The PayPal records showed that the paying account also had an email address associated with it, namely: “ald7@protonmail.com”. Notably, the three letters in this Protonmail email address, “ald,” correspond to what would be the initials of User 2’s three-word user name (which is being disguised in this affidavit) on Network 1 and Network 2. This indicated to SA Conrad that User 2 was associated with this Protonmail email account. SA Conrad’s investigation into the Network Admin Chat Room 2 logs subsequently revealed that “ald7@protonmail.com” was the same email address that User 2 had used to register his account on Network 1 and Network 2, further suggesting that User 2 was the “Joseph Lerner” who paid User 4 for maintenance of Network 2. (As will be discussed in further detail below, the investigation later revealed that “Lerner” is the maiden name of the mother of Joseph COHEN.)

24. On or about October 1, 2019, SA Conrad served a summons on PayPal seeking any information related to this Protonmail email address. PayPal responded with the following information:

Name: Joseph Lerner
CCName: ALD7
Email Address: ald7@protonmail.com
Time Created: Wed, 05 Sep 2018 17:14:16
IP address: 196.52.84.8

SA Conrad ran the 196.52.84.8 IP address through the publicly accessible American Registry for Internet Numbers (“ARIN”) and the IP address comes back to the company Logicweb, which leases IPs to other companies, including virtual private network services. SA Conrad reviewed the logs associated with Network 2 Admin Chat Room 2 for any information indicating whether IP address 196.52.84.8 had been used on the network. SA Conrad found that User 2 utilized that same IP address on the same day as the PayPal registration—September 5, 2018—and was using it while that user was connected to Chat Room 1 and Chat Room 2 on Network 2, further suggesting a connection between User 2 and the PayPal account that paid User 4 for the maintenance of Network 2.

25. As a result of the search warrants executed on August 28, 2019, several electronic devices were also seized from User 5. During a forensic review of these devices, SA Conrad found several text messages on User 5’s cell phone between User 5 and a contact named “Joseph Cohen,” with phone number “818-405-2844,” that seemed to discuss Network 2. This indicated to SA Conrad that this Joseph Cohen may also have been involved in the child exploitation conduct happening on Network 2. One such text message User 5 sent to “Joseph Cohen,” on or about December 22, 2018, at approximately 0943 hours (UTC -5), stated, “We are fucked now. My landlord spilt water on my laptop so now I have no computer at all and she doesnt have the money to replace it.” Logs recovered from that laptop’s hard drive showed that User 5 had also posted a message into the Network 2 Admin Chat Room 1 on that same day about this incident. The message, which was posted on or about December 22, 2018, at approximately 1223 hours

ET, stated, “We have a emergency. A lot. i have no laptop or computer anymore. landlord accidently spilt water on it so now it wont power on and she doesnt have the money to replace it.” The forensic review of the seized cell phone also showed that User 5 sent Joseph Cohen another text message about Network 2 on or about January 4, 2019, at approximately 1646 hours (UTC -5), which stated, “Also ive came up with a idea to better secure the [Network 2 Protocol A network] and keep it online.”

26. SA Conrad determined through his investigation that, during the December 22, 2018, and January 4, 2019, activity referenced above, T-Mobile was the cellular provider for the 818-405-2844 phone number. On or about March 19, 2020, SA Conrad sent a summons to T-Mobile for subscriber information pertaining to that number during the relevant time period. On or about April 8, 2020, T-Mobile responded, with the following subscriber information:

Name: Jacqueline A. Cohen
Subscriber Address: 10668 Angel Dreams Ave. Las Vegas, NV 89144
(SUBJECT PREMISES)
Account Number: 960046279
Activation Date: 7/6/2018
Termination Date: 5/4/2019
MSISDN Disconnect Reason: Port Out

27. After learning that the subscriber had terminated service with T-Mobile on or about May 4, 2019, SA Conrad subsequently learned that the 818-405-2844 phone number was currently being serviced by Verizon Wireless. On or about March 19, 2020, SA Conrad sent a summons to Verizon Wireless for the current subscriber information pertaining to that phone number. On or about March 25, 2020, Verizon Wireless responded with the following subscriber information (which matched the name and address contained in the T-Mobile response):

Name: Jacqueline A. Cohen
Subscriber Address: 10668 Angel Dreams Ave. Las Vegas, NV 89144
Account Number: 673545310-1
Mobile Telephone Number (MTN) Effective Date: 5/4/2019
IMEI: 351751103260850

28. On or about April 9, 2020, SA Conrad conducted a check within CLEAR, a law enforcement database that compiles public records, for address 10668 Angel Dreams Ave in Las Vegas, Nevada. CLEAR listed only two individuals that recently lived at that address: Jacqueline Cohen (DOB: XX/XX/1968) and Joseph Cohen (DOB XX/XX/1978). With regards to Joseph Cohen, CLEAR provided the following information:

Name: Joseph Cohen
Date of Birth: XX/XX/1978
SSN: XXX-XX-4855
Address: 10668 Angel Dreams Ave Las Vegas, Nevada 89144

29. After determining that COHEN's address was in Las Vegas, Nevada, SA Conrad recalled that he had previously issued a summons to PayPal for transactions related to User 5's account. PayPal had responded with transaction logs pertaining to that account. SA Conrad learned from these logs that, on or about September 7, 2018, there was a payment to User 5's account from one "donate.nxtgamingsolutions.org" in the amount of \$250. SA Conrad subsequently issued a summons to PayPal for transactions related to the "donate.nxtgamingsolutions.org" email address. PayPal responded with the transaction logs pertaining to that account. The logs showed that there was only the one transaction associated with this email address: a \$250 payment made to User 5's account with a prepaid Visa gift card issued by Bancorp Bank on or about September 7, 2018. (This was approximately two days after User 4 introduced User 2 to the Network 2 administrators as a new "financial investor," as detailed above.) SA Conrad contacted Bancorp who directed SA Conrad to Incomm Inc., a

payment technology company, in order to learn about the card's activation history. In response to his request, Incomm provided SA Conrad with the following information:

Card Number: Ending in 0203
Card Type: Vanilla Visa Int'l
Merchant Purchased: CVS Pharmacy
Merchant Address: 10400 West Charleston Boulevard Las Vegas, NV 89135
Card Activation Credit: \$250
Date/Time Card Activated: 9/7/2018 @ 2:16 PM XXX
Date/Time First Used: 9/7/2018 @ 3:51 PM (PayPal – nxtgamingsolutions)

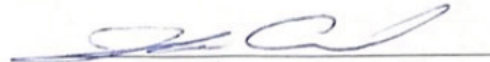
SA Conrad learned through subsequent investigation that the CVS where this gift card was purchased is approximately 2.7 miles from COHEN's address.

30. On or about March 26, 2020, SA Conrad conducted a check with the United States Department of State for any passport applications for a "Joseph Cohen" with a birth date matching the one contained in the CLEAR report. This check yielded the following information:

Name: Joseph Chaim Cohen
Address: 10668 Angel Dreams Avenue, Las Vegas, NV 89144
Date of Birth: XX/XX/1978
SSN: XXX-XX-4855
Place of Birth: Las Vegas, NV
Phone Number: 818-405-2844
Email: jcohentech@gmail.com
Mother's Maiden Name: Lerner

CONCLUSION

31. Based on the foregoing, there is probable cause to believe that Joseph COHEN has committed violations of 18 U.S.C. § 2252A(a)(2) and (b)(1) (Conspiracy to Receive and Distribute Child Pornography) and violations of 18 U.S.C §§ 2251(d) & (e) (Conspiracy to Advertise Child Pornography).



Joshua Conrad
Special Agent
Homeland Security Investigations

Subscribed to and sworn telephonically this 19th day of June 2020, and I find probable cause.



Dena Hanovice Palermo
United States Magistrate Judge

